

Remarks

In view of the above amendments and the following remarks, reconsideration of the rejections and further examination are requested.

It is noted that new claims 38-41 have been added.

Claims 19-37 have been rejected by the Examiner as being anticipated by Nonaka (US 7,073,073).

Claims 19 and 28 have been amended so as to further distinguish the present invention, as recited therein, from the reference relied upon in the above-mentioned rejection.

It is submitted that the above-mentioned rejection is not applicable to the pending claims for the following reasons.

Claim 19 is patentable over Nonaka, since claim 19 recites a playback terminal including, in part:

- a decryption method judgment unit operable to judge whether or not information managed by an external license server is required for decrypting encrypted content;

- a communication unit operable to acquire the information managed by the external license server when it is judged that the information is required; and

- a decryption unit operable to (a) decrypt the encrypted content using only medium information prerecorded on a portable medium and information pre-stored in the playback terminal itself, without using the information managed by the external license server, when it is judged that the information is not required, and (b) decrypt the encrypted content using the information acquired from the external license server when it is judged that the information is required.

It is noted that two copyright protection systems for content exist in parallel, the first copyright protection system being such that encrypted content cannot be decrypted unless rights information is obtained from an external server via a network, and the second copyright protection system being such that encrypted content can be decrypted without a network connection, using medium information pre-recorded on a medium. An example of the second copyright protection system is CSS (Contents Scrambling System), which is presently used in the Digital Versatile Disc (DVD).

In recent years, the Blu-ray Disc (BD) has appeared as a new type of media to replace the DVD. Currently, the BD uses the aforementioned second copyright protection system as its

content copyright protection system, which is similar to the DVD. On the other hand, due to the decryption method judgment unit, the communication unit and the decryption unit, as recited in claim 19, the present invention makes it possible to decrypt encrypted content when encrypted content stored on a portable medium includes both encrypted content protected by the first copyright protection system and encrypted content protected by the second copyright protection system. In addition, when encrypted content protected by the first copyright protection system is stored on a first portable medium, and encrypted content protected by the second copyright protection system is stored on a second portable medium, the present invention is able to decrypt the encrypted content stored on both recording mediums. Nonaka fails to disclose or suggest the above-mentioned features of claim 19 that make this operation of the present invention possible.

Nonaka discloses a system for distributing encrypted content data. In describing the operation of the system, Nonaka discloses that "[a]s the purchase modes of the content, there are for example a straight purchase without restriction as to reproduction by the purchaser and copying for the usage of the related purchaser and a reproduction charge charging whenever it is reproduced." (See column 46, lines 5-9). Further, Nonaka discloses that "semi-disclosure parameter data 199 is described in the usage control policy data 106 and indicates the handling of the content in the trial listening mode." (See column 47, lines 1-3). Nonaka also discloses the flow of processing of the system, which includes "Step SL8: The purchase mode of the content is determined by the purchase operation of the purchase mode determination controller 165 shown in FIG. 32 by the user, then the control signal S165 indicating the related determined purchase mode is input to the charge processor 187." (See column 52, lines 13-17). Based on these portions of Nonaka, it is apparent that the distribution system has two usage modes of the content, a "purchase mode" and a "trial listening mode."

In the rejection, it appears that the purchase mode disclosed in Nonaka is being relied upon as corresponding to the claimed decryption using the information acquired from the external license server in the present invention, and the trial listening mode in Nonaka is being relied upon as corresponding to the claimed decryption that does not use the information managed by the external license server. The rejection also appears to equate the media key data K_{MED} of Nonaka with the medium information recited in claim 19, and the key file KF of Nonaka with the information managed by the external license server recited in claim 19.

However, in the system of Nonaka, a content key K_c is required for decrypting the

content in both the purchase mode and a semi-disclosure mode (i.e., the trial listening mode). This is apparent from column 48, lines 30-64 of Nonaka which recites, in part, that "an explanation will be made of the flow of the processing in the case where the content data C having the purchase mode already determined and stored in the download memory 167 is reproduced by referring to FIG. 23 and FIG. 25" (see column 48, lines 30-64, particularly step S13 and step S14); and from column 56, lines 9-52 of Nonaka which recites, in part, that "[t]he decryptor 221 decrypts the content key data Kc, semi-disclosure parameter data 199, ..." (see column 56, lines 9-52, particularly lines 18-21).

Further, Nonaka discloses that the content key Kc is stored in the key file KF, and the key file KF is distributed in the form of a secure container by an external content provider. (See column 27, lines 14-24). Therefore, in the system of Nonaka, the key file KF is acquired from the external content provider in both the purchase mode and the trial listening mode.

Based on the above discussion of Nonaka, the encrypted content would not be able to be decrypted unless the key file KF (equated in the rejection with the information managed by the external license server recited in claim 19) was acquired from an external source even in the trial listening mode (equated in the rejection with the case in which the information managed by the external license server is not required in claim 19). Hence, it would not be possible to perform the decryption processing of the present invention that is performed in the case in which information managed by the external license server is not required, namely the decryption processing that uses only medium information pre-stored on a portable medium and information pre-stored in the playback terminal itself without communication with an external source.

It can, therefore, be seen that there are discrepancies in the correlations set forth in the rejection, and that Nonaka does not disclose the decryption method judgment unit, the communication unit, and the decryption unit as recited in claim 19. Accordingly, with the system of Nonaka, it would be possible to decrypt encrypted content protected by the first copyright protection system, but it would not be possible to decrypt encrypted content protected by the second copyright protection system. As a result, the present invention as recited in claim 19 has a superior effect due to the decryption method judgment unit, the communication unit and the decryption unit not disclosed by Nonaka, and is, therefore, patentable over Nonaka.

As for claim 28, it is patentable over Nonaka for reasons similar to those discussed above in support of claim 19. That it claim 28 recites, in part, judging whether or not information managed by an external license server is required for decrypting encrypted content; acquiring the information managed by the external license server when it is judged that the information is required; and a decryption step of (a) decrypting the encrypted content using medium information pre-recorded on a portable medium and information pre-stored in a playback terminal itself, without using the information managed by the external license server, when it is judged that the information is not required, and (b) decrypting the encrypted content using only the information acquired from the external license server when it is judged that the information is required, which features are not disclosed or suggested by Nonaka.

Claim 35 has been rejected by the Examiner as being obvious from Nonaka in view of Belenko (US 2002/0114458).

Regarding this rejection, it is submitted that claim 35 is patentable over the combination of Nonaka and Belenko for the following reasons.

Belenko discloses an invention relating to copy protection. More specifically, Belenko discloses that "[w]hen a media data set is encrypted by using a hybrid cryptographic technique, only compliant playing devices are able to play the encrypted media data set" (see paragraph [0026]), "[w]hen a compliant playing device plays an original media data set, the compliant playing device is able to embed a player watermark in the played media signal if it has a watermarking capability" (see paragraph [0027]), and "[t]he protocol provides the compliance testing between the devices through an authenticated handshaking process. If the authentication of a displaying device is not approved, the media data set should not be transferred to the displaying device" (see paragraph [0029]).

However, Belenko fails to address the deficiencies of Nonaka discussed above with respect to the features recited in claim 28 that are not disclosed or suggested by Nonaka. As a result, claim 35 is patentable over the combination of Nonaka and Belenko based at least on its dependency from claim 28.

Because of the above-mentioned distinctions, it is believed clear that claims 19-41 are allowable over the references relied upon in the rejections. Furthermore, it is submitted that the distinctions are such that a person having ordinary skill in the art at the time of invention would not have been motivated to make any combination of the references of record in such a manner as to result in, or otherwise render obvious, the present invention as recited in claims 19-41. Therefore, it is submitted that claims 19-41 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The Examiner is invited to contact the undersigned by telephone if it is felt that there are issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Masaya YAMAMOTO et al.

By: /David M. Ovedovitz/
2008.08.18 16:19:12 -04'00'

David M. Ovedovitz
Registration No. 45,336
Attorney for Applicants

DMO/jmj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 18, 2008